UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/749,042	12/30/2003	Jon C. Graff	042933/272518	9223

826 7590 05/17/2007

ALSTON & BIRD LLP
BANK OF AMERICA PLAZA
101 SOUTH TRYON STREET, SUITE 4000
CHARLOTTE, NC 28280-4000

EXAMINER	
LE, NANCY LOAN T	
ART UNIT	**PAPER NUMBER**
3621	

MAIL DATE	DELIVERY MODE
05/17/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/749,042	GRAFF, JON C.	
	Examiner	Art Unit	
	NANCY T. LE	3621	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 July 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-18* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-18* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Acknowledgements

1. This action is responsive to Amendment filed 20 July 2006 in which no claim has been amended, canceled or added.

2. This paper is assigned Paper No. 20070511 by the Examiner.

Status of Claims

3. Claims 1-18 have been examined.

Response to Arguments

4. Applicant's arguments filed 20 July 2006 with respect to claims 1-18 have been fully considered but they are not persuasive. The Applicant contends that the prior art (Ozog et al., US 2003/0033528 A1) does not teach or suggest *(i) a secondary certification authority (CA) providing* ***role certificate****(s) to a terminal based upon position(s) of the terminal within an organization; (ii) a tertiary CA providing* ***permission certificate*** *to the terminal based upon characteristic(s) of the terminal at a position in the organization; or (iii) a server* ***authenticating*** *the terminal based upon an identity certificate, the role certificate(s) and the permission certificate(s).* However, the Office respectfully disagrees because since the Applicant does not lexicographically define the term '***capable of***', the Office relies on the ordinary meaning of the term. According to Merriam-Webster dictionary, '***capable of***' means "having or showing general efficiency and/or **ability**". As such, the Office interprets "*a terminal* ***capable of*** *communicating at least one of within and across at least one network ...* ", "*a secondary certification authority (CA)* ***capable***

***of** providing **role certificate**(s) to a terminal based upon position(s) of the terminal within an organization ...", "a tertiary CA **capable of** providing **permission certificate** to the terminal based upon characteristic(s) of the terminal at a position in the organization", and "a server **authenticating** the terminal based upon an identity certificate, the role certificate(s) and the permission certificate(s)"* (see claims 1, 7) to be "a terminal **having the ability to** communicate ...", "a secondary certification authority (CA) **having the ability to** provide **role certificate**(s) to a terminal based upon position(s) of the terminal within an organization ... ", "a tertiary CA **having the ability to** provide **permission certificate** to the terminal based upon characteristic(s) of the terminal at a position in the organization ...", and "a server **having the ability to authenticate** the terminal based upon an identity certificate, the role certificate(s) and the permission certificate(s) ...", and do *not* actually communicate, provide and authenticate. As per the Ozog reference, it shows a terminal (such as *computer desktop* **[0056]**) communicating in a network (**fig. 8**) ..., therefore, Ozog shows a computer/terminal capable of communicating in a network. Similarly, Ozog shows (i) a secondary CA (such as the certificate authority of the Issuer/Grantor's company, the Telecommunication Service Provider V, or public authority such as 'Mandate Authority 410, 510' (**[0065], figs. 4, 5**)) providing a role certificate (such as the '*Issuer/Grantor Certified Reference*' **[0041-0042, 0054, 0059, 0110]**) ..., therefore, Ozog shows a secondary CA *capable of* providing a role certificate ...; (ii) a tertiary CA (such as the Issuer/Grantor B Virtual Certificate Authority VCA(B) **[0062, 0065]**) providing permission certificate (such as *Mandate* to the terminal ... **[0032, 0033, 0043, 0066]**), therefore, Ozog shows a tertiary CA *capable of* providing a permission certificate ...; and (iii) a server (such as a computer system owned by third-party or service provider V **[0110]**) authenticating the terminal based upon an identity certificate (such as the public-key certificate from the certificate authority CA(X), authenticity certificate 512 **[0063, 0074]**), the role certificate(s) (such as the VCA(B) **[0067-0068]**) and the permission certificate(s) (such as Mandate **[0033, 0071]**) of the terminal ..., therefore, Ozog shows a server *capable of* authenticating a terminal based upon an identity certificate, role certificate, permission certificate ...; and hence, Ozog have the claim limitations.

5. If applicant wants to claim the aspects of communicating in a network, providing certificate(s) and authenticating a terminal, the applicant should revise the claims to reflect these communicating, providing and authenticating aspects.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. §102 that form the basis for the rejections under this section made in this Office action:

> *A person shall be entitled to a patent unless –*
>
> *(a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.*

7. Claims 1-18 are rejected under 35 U.S.C. §102(a) as being anticipated by U.S. Patent Application Publication No. **2003/0033528 A1** published 13 February 2003 to **Ozog et al.**.

8. As per **claim 1**, Ozog et al. disclose a system comprising:

- **a terminal** *capable of* communicating at least one of within and across at least one network, wherein the terminal is included within an organization including a plurality of terminals, at least one terminal having at least one characteristic and being at least one of a plurality of positions within the organization (Since the Applicant does not lexicographically define the term '***capable of***', the Office relies on the ordinary meaning of the term. According to Merriam-Webster dictionary, '***capable of*** means "*having or showing general efficiency and/or* ***ability***". As such, the Office interprets "*a terminal* ***capable of*** *communicating at least one of within and across at least one network ...* " to be "a terminal **having the ability to** communicate ...", and do *not* actually communicate .... Ozog shows a terminal such as

computer desktop **[0056]** communicating in a network **(fig. 8)** …, therefore, Ozog shows a computer/terminal capable of communicating in a network);

- **a secondary certification authority** (CA) *capable of* providing at least one role certificate to the terminal based upon the at least one position of the terminal within the organization, wherein the organization includes a plurality of secondary CA's capable of issuing at least one role certificate to respective groups of terminals of the organization (With similar interpretation and reasoning as above, Ozog shows a secondary certification authority {such as the *certificate authority of the Issuer/Grantor's company, the Telecommunication Service Provider V, or public authority such as Mandate Authority 410, 510* – para. **[0065], figures 4, 5**} providing a role certificate {such as the '*Issuer/Grantor Certified Reference*' **[0041-0042, 0054, 0059, 0110]**} …, therefore, Ozog shows a secondary CA *capable of* providing a role certificate);

- **a tertiary CA** *capable of* providing at least one permission certificate to the terminal based upon the at least one characteristic of the terminal that is located at a position within the organization, wherein the organization includes a plurality of tertiary CA's capable of issuing at least one permission certificate to respective sub-groups of terminals of the organization (With similar interpretation and reasoning as above, Ozog shows a tertiary certification authority {such as the *Issuer/Grantor B Virtual Certificate Authority VCA(B)* – para. **[0062, 0065]**} providing a permission certificate {such as the '*Mandate*' – para. **[0032, 0033, 0043, 0066, 0071]**} …, therefore, Ozog shows a tertiary CA *capable of* providing at least one permission certificate to the terminal …); and

- **a server** *capable of* authenticating the terminal based upon an identity certificate, the at least one role certificate, and the at least one permission certificate of the terminal to thereby determine whether to grant the terminal access to at least one resource of the server (With similar interpretation and reasoning as above, Ozog shows a server {such as a *computer system owned by third-party or service provider V* – para. **[0110]**} authenticating the terminal based upon an identity certificate {such as *public key certificate from certificate authority CA(X), authenticity certificate 512* – para. **[0063, 0074]**}, a role certificate {such as *the VCA(B) certificate* – para. **[0067-0068]**}, a permission certificate {such as the '*Mandate*' – para. **[0032, 0033, 0043, 0066, 0071]**} of the terminal to thereby determine whether to grant the terminal/entity access to at least one resource of the server {such as *access to the electronic document* – para. **[0072-0079, 0106]**}, therefore, Ozog shows a server *capable of* authenticating the terminal based upon an identity certificate, the at least one role certificate, and the at least one permission certificate of the terminal ...).

9. As per **claims 2, 3, 8 and 9**, Ozog et al. disclose a system/method of claims 1 and 7, respectively, wherein the terminal comprises a terminal included within an organization comprising a customer base of a cellular service provider that includes a plurality of terminals, each terminal being at one of a plurality of positions comprising a plurality of 'service plans'/services offered by the cellular network operator, and wherein at least one terminal has at least one characteristic comprising at least one optional service offered by the cellular network operator **[0080, 0105-0107]**.

10. As per **claims 4 and 10**, Ozog et al. disclose a system/method of claims 1 and 7, respectively, wherein the tertiary CA is *capable of* providing at least one permission certificate each having an associated validity time no greater than a validity time of the at least one role certificate provided by the

secondary CA, and no greater than a validity time of the identity certificate (**[0044, 0057, 0075-0077, 0106]** with similar interpretation and reasoning about '*capable of*' as detailed in claim 1 above).

11. As per **claims 5 and 11**, Ozog et al. disclose a system/method of claims 4 and 10, respectively, wherein the server is *capable of* authenticating the terminal based upon the validity times of the identity certificate, at least one role certificate and at least one permission certificate of the respective terminal (**[0075-0079, 0106]** with similar interpretation and reasoning about '*capable of*' as detailed in claim 1 above).

12. As per **claims 6 and 12**, Ozog et al. disclose a system/method of claims 1 and 7, respectively, wherein the terminal is *capable of* requesting access to at least one resource of a server before the server authenticates the terminal (para. **[0071, 0072, 0099]** with similar interpretation and reasoning about '*capable of*' as detailed in claim 1 above), and wherein the server is capable of granting access to the at least one resource if the terminal is authenticated (para. **[0079]** with similar interpretation and reasoning about '*capable of*' as detailed in claim 1 above).

13. As per **claim 7**, Ozog et al. disclose a method of authenticating a terminal comprising:

- providing a terminal *capable of* communicating at least one of within and across at least one network, wherein the terminal is included within an organization including a plurality of terminals, at least one terminal having at least one characteristic and being at least one of a plurality of positions within the organization (see claim 1 for interpretation, reasoning and citation);

- providing at least one role certificate to the terminal from a secondary certification authority (CA) based upon the at least one position of the terminal within the organization, wherein the

organization includes a plurality of secondary CA's capable of issuing at least one role certificate to respective groups of terminals of the organization (see claim 1 for interpretation, reasoning and citation);

- providing at least one permission certificate to the terminal from a tertiary CA based upon the at least one characteristic of the terminal located at a position within the organization, wherein the organization includes a plurality of tertiary CA's *capable of* issuing at least one permission certificate to respective sub-groups of terminals of the organization (see claim 1 for interpretation, reasoning and citation); and

- authenticating the terminal at a server based upon an identity certificate, the at least one role certificate and the at least one permission certificate of the terminal to thereby determine whether to grant the terminal access to at least one resource of the server (see claim 1 for interpretation, reasoning and citation).

14. As per **claim 13**, Ozog et al. disclose a terminal included within an organization including a plurality of terminals, each terminal having at least one characteristic and being at least one of a plurality of positions within the organization, the terminal comprising:

- **a controller** *capable of* communicating at least one of within and across at least one network, wherein the controller is *capable of* obtaining at least one role certificate 10 from a secondary certification authority (CA) based upon the at least one position of the terminal within the organization and at least one permission certificate from a tertiary CA based upon the at least one characteristic of the terminal that is located at a position within the organization, wherein the organization includes a plurality of secondary CA's *capable of* issuing at least one role certificate to respective groups of terminals of the organization, and wherein the organization

includes a plurality of tertiary CA's *capable of* issuing at least one permission certificate to respective sub-groups of terminals of the organization (i.e., a controller is implicitly included in computing platforms of para. [0027] or in computer desktops of para. [0056]; the controller has the ability of obtaining an Issuer/Grantor Certified Reference {a role certificate} – para. **[0041-0042, 0054, 0059, 0110]** from a certificate authority of the Issuer/Grantor's company, the Telecommunication Service Provider V, or public authority such as Mandate Authority 410, 510 {secondary certificate authority} – para. **[0065], figures 4, 5**; and obtaining a Mandate {permission certificate} -- para. **[0032, 0033, 0043, 0066, 0071]** from Issuer/Grantor B Virtual Certificate Authority VCA(B) {tertiary CA} – para. **[0062, 0065]**. Also see claim 1 for interpretation and reasoning); and

- **a memory** *capable of* storing an identity certificate, at least one role certificate and at least one permission certificate **[0056]**,
- wherein the controller is also *capable of* communicating with a server (i.e., the controller of the terminal/'computing platform' requesting access to a controlled resource on the third-party, or Telecommunication Service Provider V – para. **[0071, 0072, 0099]**) such that the server is *capable of* authenticating the terminal based upon the identity certificate, the at least one role certificate and the at least one permission certificate of the terminal to thereby determine whether to grant the terminal access to at least one resource of the server (para. **[0072-0079, 0106]**. Also see claim 1 for interpretation and reasoning).

15. As per **claim 14**, Ozog et al. disclose a terminal of claim 13, wherein the controller is capable of obtaining at least one role certificate from a secondary CA *capable of* issuing at least one role certificate to each terminal of the organization comprising a customer base of a cellular service provider that includes a plurality of terminals, each terminal being at one of a plurality of positions comprising a plurality

of service plans offered by the cellular network operator, and wherein the controller is *capable of* obtaining at least one permission certificate based upon at least one characteristic comprising at least one optional service offered by the cellular network operator (i.e., a controller is implicitly included in computing platforms of para. [0027] or in computer desktops of para. [0056]; the controller capable of obtaining an Issuer/Grantor Certified Reference {a role certificate} – para. **[0041-0042, 0054, 0059, 0110]** from a certificate authority of the Issuer/Grantor's company, the Telecommunication Service Provider V, or public authority such as Mandate Authority 410, 510 {secondary certificate authority} – para. **[0065]**, **figures 4, 5**; and obtaining a Mandate {permission certificate} -- para. **[0032, 0033, 0043, 0066, 0071]** from Issuer/Grantor B Virtual Certificate Authority VCA(B) {tertiary CA} – para. **[0062, 0065]**. Also see claim 1 for interpretation and reasoning).

16. As per **claim 15**, Ozog et al. disclose a terminal of claim 13, wherein the controller is *capable of* obtaining at least one role certificate from a secondary CA *capable of* issuing at least one role certificate to each terminal of the organization comprising a customer base of a cellular service provider that includes a plurality of terminals, each terminal being at least one of a plurality of positions comprising a plurality of services offered by the cellular network operator, and wherein the controller is *capable of* obtaining at least one permission certificate based upon at least one characteristic comprising at least one optional service offered by the cellular network operator (i.e., a controller is implicitly included in computing platforms of para. [0027] or in computer desktops of para. [0056]; the controller capable of obtaining an Issuer/Grantor Certified Reference {a role certificate} – para. **[0041-0042, 0054, 0059, 0110]** from a certificate authority of the Issuer/Grantor's company, the Telecommunication Service Provider V, or public authority such as Mandate Authority 410, 510 {secondary certificate authority} – para. **[0065]**, **figures 4, 5**; and obtaining a Mandate {permission certificate} – para. **[0032, 0033, 0043, 0066, 0071]** from Issuer/Grantor B Virtual Certificate Authority VCA(B) {tertiary CA} – para. **[0062, 0065]**. Also see claim 1 for interpretation and reasoning).

17. As per **claim 16**, Ozog et al. disclose a terminal of claim 13, wherein the controller is *capable of* obtaining at least one permission certificate each having an associated validity time no greater than a validity time of the at least one role certificate obtained by the controller, and no greater than a validity time of the identity certificate (**[0044, 0057, 0075-0077, 0106]**. Also see claim 1 for interpretation and reasoning about 'capable of').

18. As per **claim 17**, Ozog et al. disclose a terminal of claim 16, wherein the controller is also *capable of* communicating with a server (para. **[0071, 0072, 0099]**) such that the server is *capable of* authenticating the terminal based upon the validity times of the identity certificate, at least one role certificate and at least one permission certificate of the respective terminal (para. **[0075-0079, 0106]**. Also see claim 1 for interpretation and reasoning).

19. As per **claim 18**, Ozog et al. disclose a terminal of claim 13, wherein the controller is *capable of* requesting access to at least one resource of a server before the server authenticates the terminal (para. **[0071, 0072, 0099]**) such that the server is capable of granting access to the at least one resource if the terminal is authenticated (para. **[0079]**. Also see claim 1 for interpretation and reasoning).

Conclusion

20. Examiner has pointed out particular references contained in the prior arts of record in the body of this action for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant, in preparing the response, to consider fully the entire references as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the examiner.

21. **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

22. A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

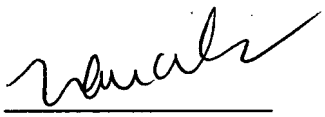
23. Any inquiry of a general nature or relating to the status of this application or concerning this communication or earlier communications from the examiner should be directed to NANCY LOAN T. LE whose telephone number is **(571) 272-7066**. The examiner can normally be reached on Monday - Friday, 9am - 6:00pm Eastern Standard Time.

24. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, ANDREW J. FISCHER can be reached on **(571) 272-6779**.

25. For ***official/regular communication***, the fax number for the organization where this application or proceeding is assigned is ***(571) 273-8300***.

26. For **informal/draft communication**, the fax number is ***(571) 273-7066 (Rightfax)***.

27. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see **http://pair-direct.uspto.gov**. Should you have questions on access to the Private PAIR system, contact the **Electronic Business Center (EBC)** at **866-217-9197 (toll-free)**.



11 May 2007

Nancy Le

Patent Examiner

11 May 2007

ANDREW J. FISCHER
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 3600